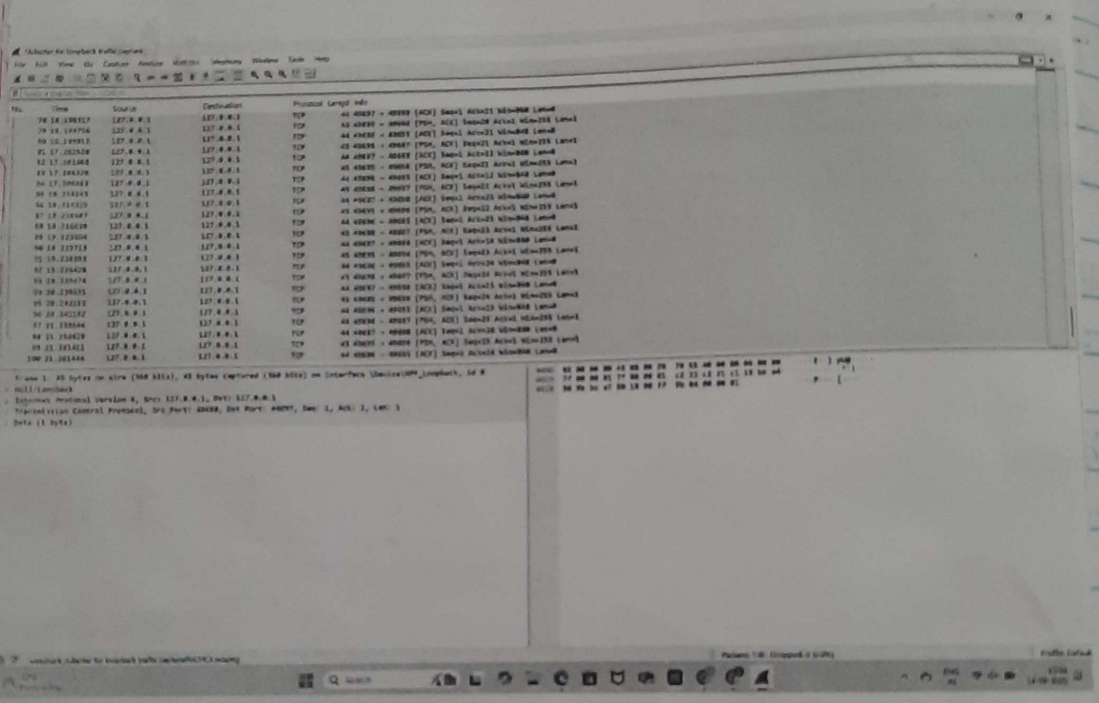
Exc 4: Experiments on Packet Capture tool: Wireshark

Aim: To understand the features of wireshark as a packet capture tool and understand encapsulation of information.



1. Create a filter to display only TCP/UDP packets, inspect the packets and provide the flow graph.

Procedure:

→ Select Local Area Connection in wireshark.

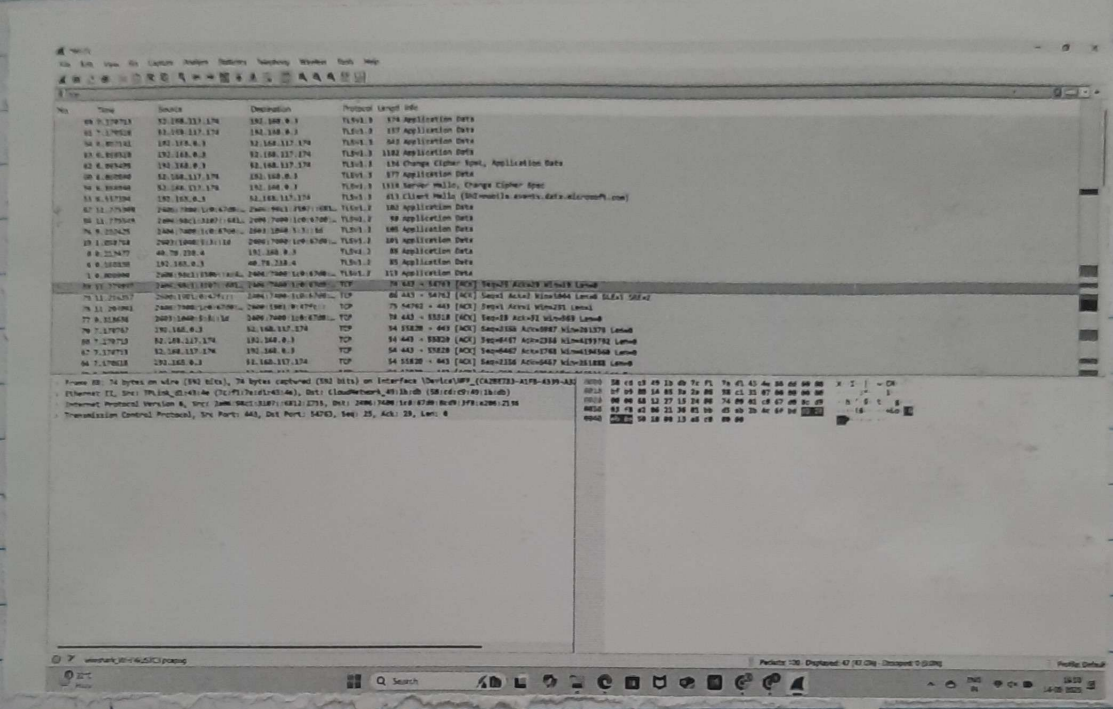
→ Go the capture → Option

→ Select stop capture automatically after 100 packets

apsara

Date

→ Then click Start capture
→ Search TCP packets in search bar.
→ To see flow graph click statistics →
Flow graph
~~→ To see flow g~~
→ Save the packets



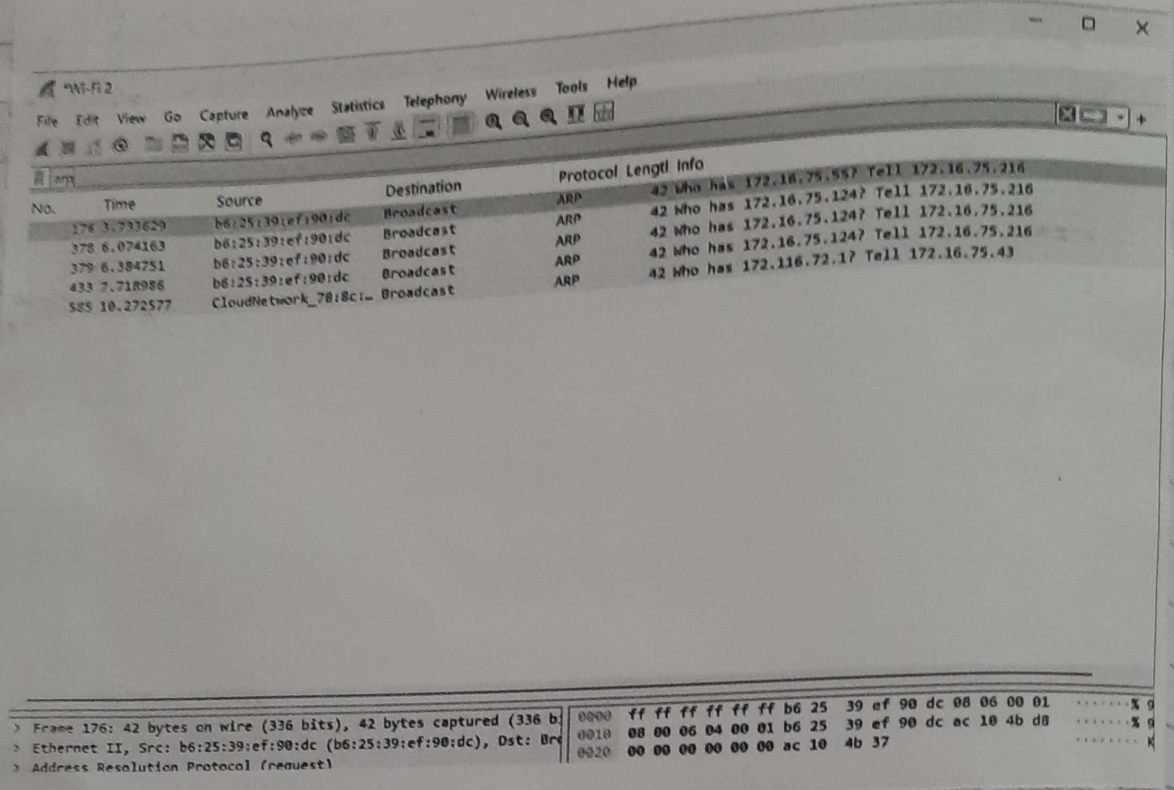
25

2. Create a filter to display only ARP packets and inspect the packets

Procedure

→ Go to capture → option
→ select stop capture automatically after 100 packets
→ Then click start capture
→ Search ARP packets in search bar

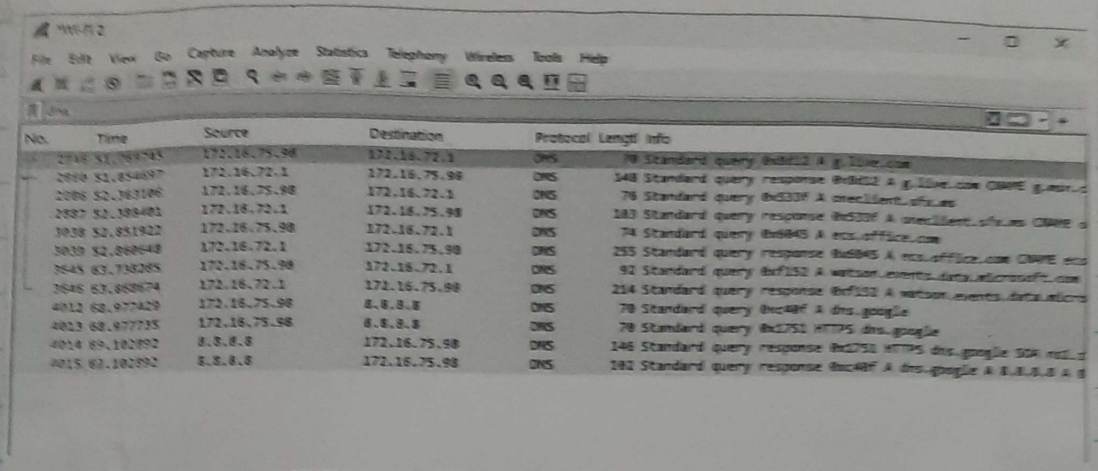
⇒ Save the packet.



40

3. Create a filter to display only DNS packets and provide the flow graph procedure.

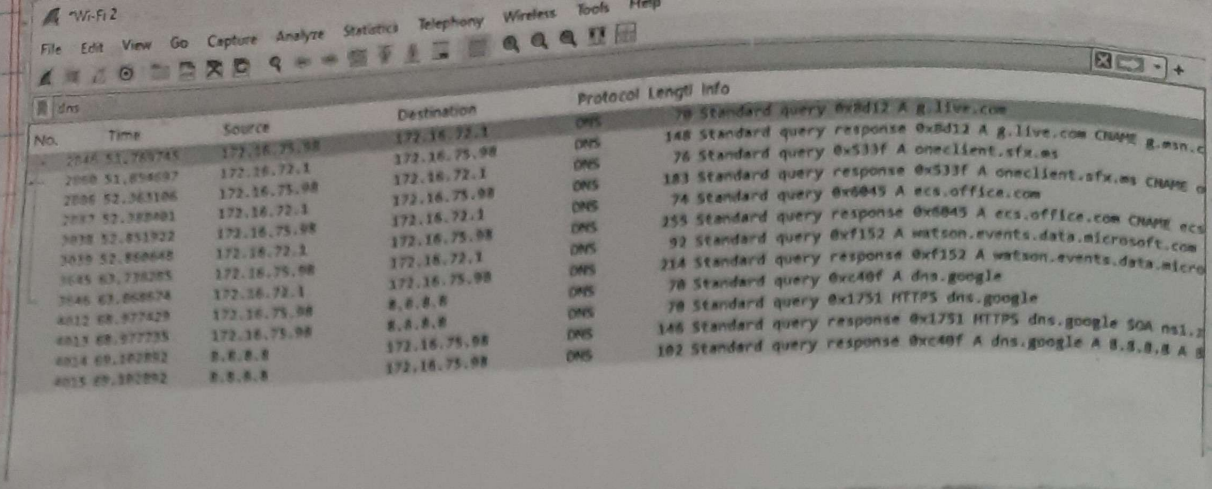
→ Go to capture → Option
⇒ Select stop capture automatically after 100 packets
⇒ Then click start capture
⇒ Search DNS packets in search bar
⇒ To see flow graph click, statistics → Flow graph.
⇒ Save the packets.



4. Create a filter to display only HTTP packets and inspect the packets

procedure:

→ Select Local Area Connection in wireshark
→ Go to capture → Option
→ Select stop capture automatically after 100 packets
→ Search - HTTP packets in Search bar
→ Save the packets



6)

5) Create a filter to display only IP/ICMP packets and inspect the packets

Procedure:

⇒ Select local Area Connection in Wireshark

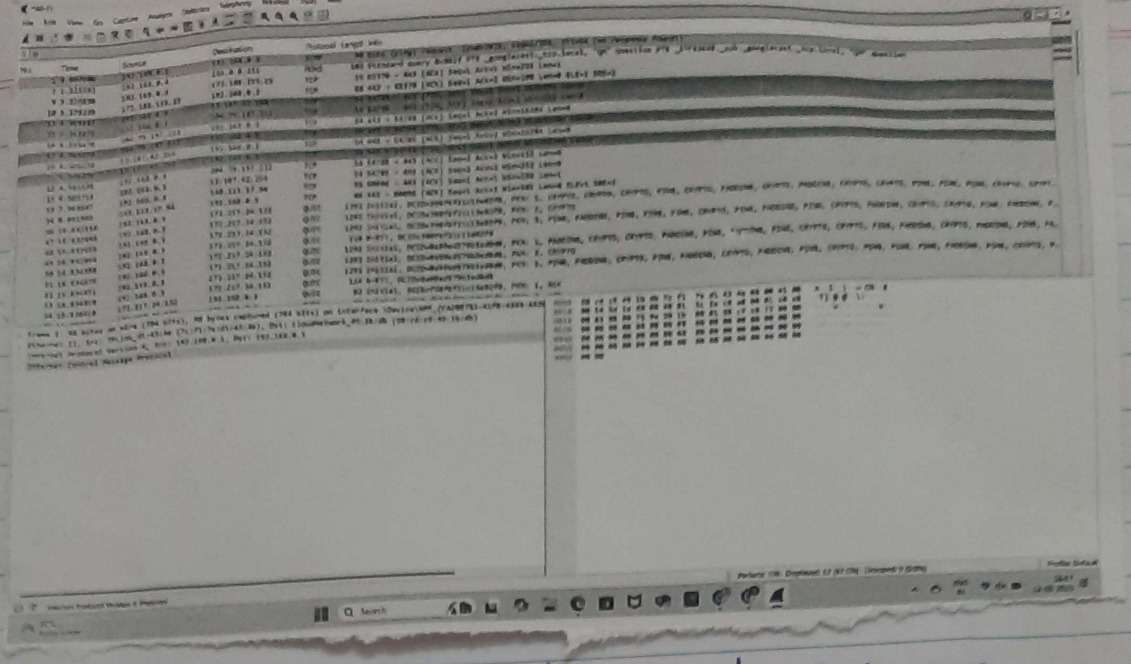
↪ Go to capture → Option

→ Select stop capture automatically after 100 packets.

→ then click Start capture

⇒ Search ICMP/IP packets in search bar.

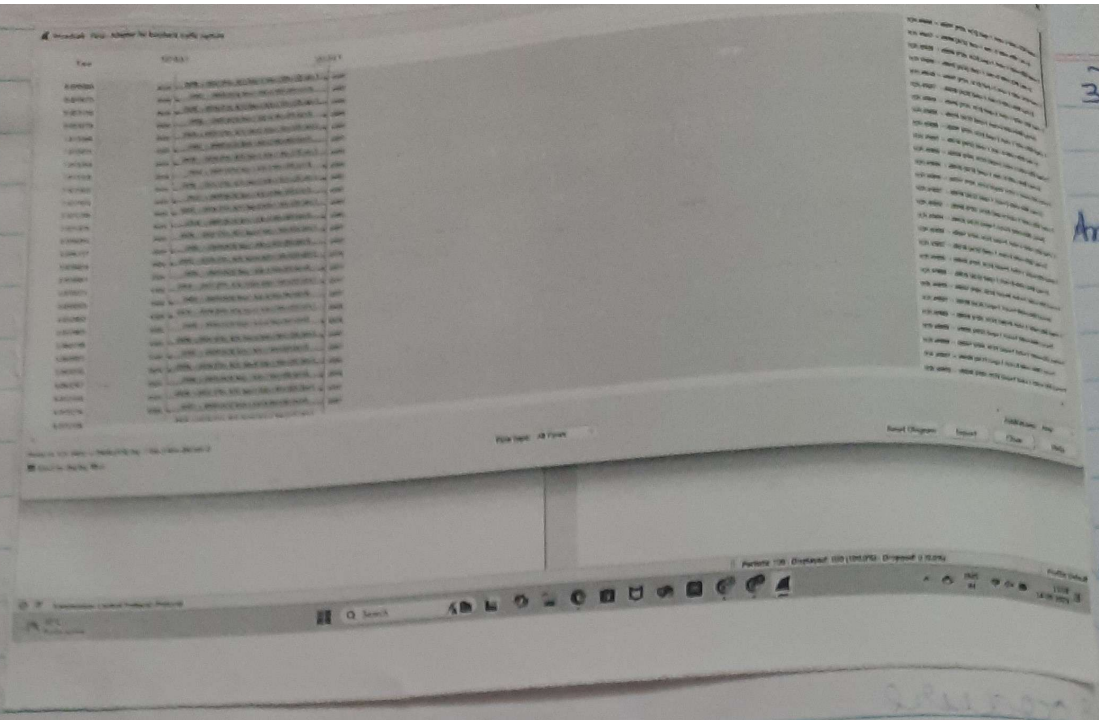
→ Save the packets



6) Create a filter to display only DHCP. packets and inspect the packets

Procedure

→ Select Local Area connection in wireshark
→ Go to capture → Option
→ Select stop capture automatically after 100 packets
→ Then click start capture
→ Search DHCP packets in search bar
→ Save the packets



Student Observation:-

1) What is promiscuous mode?

Ans: A network interface mode where a device captures all network traffic it sees, not just packets address to it.

2) Does ARP packets have transport layer header? Explain

Ans: ARP packets and transport layer header: ARP packets do not have a transport layer header. They operate at the link layer (layer 2) and are used to map IP address to MAC address without involving transport layer protocol link TCP or UDP.

3) Which ... by DN...

Ans DNS ... respons... respon...

4) What ... http

Ans: http ...

5) What ...

Ans: A ... send ... typic... subn... netw...

3) Which transport layer protocol is used by DNS?

Ans DNS primarily uses UDP for queries and responses, but can use TCP for large responses or zone transfers

4) What is the port number used by http protocol?

Ans: http uses port 80

5) What is broadcast IP address?

Ans: A broadcast IP address is used to send data to all devices in a network, typically the last address in a subnet (eg; 192.168.1.255 for 192.168.1.0/24) network

Result:

Thus experiment is performed in wireshark. is impl